ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

European Journal of Combinatorics 28 (2007) 754–761

European Journal of Combinatorics

www.elsevier.com/locate/ejc

Integer-valued polynomials on prime numbers and logarithm power expansion

Jean-Luc Chabert

Department of Mathematics, Lamfa UMR CNRS 6140, University of Picardie, 33 rue Saint Leu, 80039 Amiens, France

Received 12 January 2004; accepted 19 December 2005
Available online 28 February 2006

Abstract

We prove that two sequences arising from two different domains are equal. The first one, $\{d(n)\}_{n\in\mathbb{N}}$, comes from the following power expansion:

$$\left(-\frac{\ln(1-x)}{x}\right)^m = \left(\sum_{k=1}^{+\infty}\frac{x^k}{k+1}\right)^m = \sum_{n=0}^{\infty}\frac{B_n(m)}{d(n)}x^n$$

where $B_n(X)$ is a primitive polynomial of $\mathbb{Z}[X]$. The second sequence, $\{e(n)\}_{n\in\mathbb{N}}$, is the factorial sequence of the set of prime numbers or, equivalently, $e(n)$ is the denominator of the polynomials of degree $\leq n+1$ that take integral values for all prime numbers.

1. Introduction

If we look for integer sequences beginning with

1, 2, 24, 48 . . . ,

the *On-Line Encyclopedia in Integer Sequences* [4] gives us three sequences: A002552, A053657 and A075265. They all three continue with 5760 and 11520, that is, the three sequences begin with

1, 2, 24, 48, 5760, 11 520, ...

E-mail address: jean-luc.chabert@u-picardie.fr.

0195-6698/$ - see front matter
doi:10.1016/j.ejc.2005.12.009

Then, the first one ('denominators of coefficients for numerical differentiation') differs from the others which go on with the same computed terms:

$$1, 2, 24, 48, 5760, 11\,520, 2\,903\,040, 5\,806\,080, 1\,393\,459\,200, \ldots.$$

The aim of this paper is to answer positively to a question posed by Paul D. Hanna in [4] by proving that Sequences A053657 and A075265 are really the same.

On the one hand, the element $e(n)$ of the sequence A053657 is the common denominator of the polynomials of degree $\leq n+1$ that take integral values on the set $\mathbb{P}$ of prime numbers [3], in other words, $\frac{1}{e(n)}$ is a generator of the fractional ideal formed by the leading coefficients of the polynomials belonging to the $\mathbb{Z}$-module

$$\mathrm{Int}_{n+1}(\mathbb{P}, \mathbb{Z}) = \{f(X) \in \mathbb{Q}[X] \mid \deg(f) \leq n+1,\ f(\mathbb{P}) \subseteq \mathbb{Z}\}.$$

The element $e(n)$ may also be interpreted as the $n+1$-th factorial of the set $\mathbb{P}$ of prime numbers: $e(n)$ is the G.C.D. of all the products $\prod_{0\leq i<j\leq n+1}(p_j - p_i)$ for all $p_0, p_1, \ldots, p_{n+1} \in \mathbb{P}$ divided by the G.C.D. of all the products $\prod_{0\leq i<j\leq n}(p_j - p_i)$ [1, Theorem 10]. There is an explicit formula that gives the value of $e(n)$ (see [2] or [3]):

$$e(n) = (n+1)!_{\mathbb{P}} = \prod_{p\in\mathbb{P}, p\leq n+1} p^{\omega_p(n)} \quad \text{with } \omega_p(n) = \sum_{k\geq 0}\left[\frac{n}{(p-1)p^k}\right].$$

On the other hand, the element $d(n)$ of the sequence A075265 is defined by Paul D. Hanna [4] as the least common multiple of denominators of the coefficients of x^n, for all integer m, in the power expansion of

$$\left(-\frac{\ln(1-x)}{x}\right)^m.$$

In fact, this formulation is misleading: let us consider the following equalities between power series

$$\left(-\frac{\ln(1-x)}{x}\right)^m = \left(\sum_{k=1}^{+\infty}\frac{x^k}{k+1}\right)^m = 1 + \frac{m}{2}x + \frac{m(3m+5)}{24}x^2 + \frac{m(m^2+5m+6)}{48}x^3 + \cdots.$$

For instance, look at the sequence formed by the coefficients of x^2:

$$\left\{\frac{m(3m+5)}{24}\right\}_{m\in\mathbb{N}} = \frac{1}{3}, \frac{11}{12}, \frac{7}{4}, \frac{17}{6}, \ldots.$$

Although the least common multiple of the denominators of the numerical sequence is 12 (because, as soon as we replace m by an integer, the numerator is even), the denominator of the polynomial formula with respect to the indeterminate m is 24. The correct formulation seems to need a formal expression, like those given in the following theorem.

Theorem 1.1. *For each $m \in \mathbb{N}$, consider the power expansion:*

$$\left(\sum_{k=1}^{+\infty}\frac{x^k}{k+1}\right)^m = \sum_{n=0}^{+\infty} A_n(m)x^n.$$

The coefficient of x^n is a polynomial in m of degree n that we may write as

$$A_n(m) = \frac{1}{d(n)} B_n(m)$$

where $B_n(m)$ is a primitive polynomial in $\mathbb{Z}[m]$. Then, the denominator $d(n)$ is equal to the $n+1$-th factorial of $\mathbb{P}$, that is:

$$d(n) = \prod_{p\in\mathbb{P}, p\le n+1} p^{\omega_p(n)}$$

where

$$\omega_p(n) = \sum_{k\ge 0} \left[\frac{n}{(p-1)p^k}\right].$$

One verifies easily by induction on n that $A_n(m)$ is a polynomial function of m with degree n. More precisely, the equality

$$A_n(m+1) = \sum_{h=0}^{n} \frac{1}{n-h+1} A_h(m)$$

shows by means of the induction hypothesis that $A_n(m+1) - A_n(m)$ is a polynomial in m of degree $n-1$. Theorem 1.1 results from Lemmas 2.1, 3.5 and 3.6 below.

2. Notation

By identification of the coefficients, one has:

$$A_n(m) = \sum_{\substack{(i_1,\dots,i_m)\in\mathbb{N}^m \\ i_1+\cdots+i_m=n}} \prod_{j=1}^{m} \frac{1}{i_j+1}.$$

The i_j's may have the same value $i \in \{1,\dots,n\}$. Denoting by u_i (≥ 0) the number of i_j with value i, we obtain in the previous product an expression such that:

$$\prod_{i=1}^{n} \frac{1}{(i+1)^{u_i}}$$

which corresponds to a decomposition of n of the form:

$$u_1 + 2u_2 + \cdots + nu_n = n.$$

The number of such a decomposition of n is:

$$C_m^{u_1} C_{m-u_1}^{u_2} C_{m-(u_1+u_2)}^{u_3} \cdots C_{m-(u_1+\cdots+u_{n-1})}^{u_n} = \frac{m(m-1)\cdots(m-(u_1+\cdots+u_n)+1)}{u_1!u_2!\cdots u_n!}$$

(the C_k^l's are assumed to be equal to zero when $l > k$ and the only products to consider correspond to $u_1+\cdots+u_n \le m$). Consequently,

$$A_n(m) = \sum \left(\prod_{i=1}^{n} \frac{1}{u_i!(i+1)^{u_i}}\right) m(m-1)\cdots(m-(u_1+\cdots+u_n)+1)$$

where the sum corresponds to all the $(u_1, \dots, u_n) \in \mathbb{N}^n$ such that

$$u_1 + 2u_2 + \cdots + nu_n = n.$$

Notation. From now on, to make notation simpler we consider an integer n that is assumed to be fixed. Let

$$U = \{\underline{u} = (u_1, \dots, u_n) \in \mathbb{N}^n \mid u_1 + 2u_2 + \cdots + nu_n = n\}$$

and, for each $\underline{u} \in U$, let

$$d(\underline{u}) = \prod_{i=1}^{n} u_i!(i+1)^{u_i} \quad \text{and} \quad \sigma(\underline{u}) = u_1 + \cdots + u_n.$$

Then,

$$A_n(m) = \sum_{\underline{u} \in U} A(\underline{u}, m)$$

where

$$A(\underline{u}, m) = \frac{1}{d(\underline{u})} m(m-1)\cdots(m-\sigma(\underline{u})+1)$$

is a polynomial in m of degree $\sigma(\underline{u})$.

Notation. For each prime number p, denote by v_p the p-adic valuation of $\mathbb{Q}$ and let

$$\mu_p = \max_{\underline{u} \in U} v_p(d(\underline{u})), \quad U_p = \{\underline{u} \in U \mid v_p(d(\underline{u})) = \mu_p\}$$

$$\sigma_p = \max_{\underline{u} \in U_p} \sigma(\underline{u}), \quad \tilde{U}_p = \{\underline{u} \in U_p \mid \sigma(\underline{u}) = \sigma_p\}.$$

Clearly, if $p \in \mathbb{P}$ is such that $p > n+1$, then $v_p(d(\underline{u})) = 0$ for every $\underline{u} \in U$, and then, $v_p(d(n)) = 0$. We are going to see that, for a fixed $p \leq n+1$, among the polynomials $A(\underline{u}, m)$ such that $v_p(d(\underline{u})) = \mu_p$, there is only one polynomial of maximal degree σ_p (Lemma 3.5 below). Moreover, the maximal value μ_p of $v_p(d(\underline{u}))$ is equal to $\omega_p(n)$ (Lemma 3.6 below). The following lemma shows that Theorem 1.1 will then be proved.

Lemma 2.1. *If $\tilde{U}_p$ contains only one element, then $v_p(d(n)) = \mu_p$.*

Proof. Let us write

$$A_n(m) = \sum_{\underline{u} \in U_p} A(\underline{u}, m) + \sum_{\underline{u} \in U \setminus U_p} A(\underline{u}, m).$$

It follows from the assumption on $\tilde{U}_p$ that the first sum is of the form $\frac{1}{cp^{\mu_p}} C(m)$ where $C(m)$ is a monic polynomial in $\mathbb{Z}[X]$ and $c \in \mathbb{Z}\setminus p\mathbb{Z}$. By definition of $U\setminus U_p$, the second sum is of the form $\frac{1}{dp^{\mu_p - \delta}} D(m)$ where $D(m) \in \mathbb{Z}[X]$, $d \in \mathbb{Z}\setminus p\mathbb{Z}$ and $\delta \in \mathbb{N}^*$. Consequently,

$$\frac{1}{d(n)} B_n(m) = A_n(m) = \frac{1}{p^{\mu_p}} \frac{1}{cd} (dC(m) + cp^{\delta} D(m)) = \frac{1}{p^{\mu_p}} E(m)$$

where $E(m)$ is a primitive polynomial in $\mathbb{Z}_{(p)}[m]$. Finally, $v_p(d(n)) = \mu_p$. □

3. Uniqueness of the maximum

We still assume that n is a fixed integer and that p is a fixed prime number such that $p \leq n+1$. We are going to prove that the hypothesis of Lemma 2.1 is satisfied. Note first that, for every $\underline{u} \in U$, one has:

$$v_p(d(\underline{u})) = \sum_{i=1}^{n} [v_p(u_i!) + u_i v_p(i+1)].$$

Lemma 3.1. *For every $\underline{u} \in U$ and every $i \in \{1, \ldots, n\}$, there exists some $\underline{u}^* \in U$ such that*

$$v_p(d(\underline{u}^*)) - v_p(d(\underline{u})) \geq u_i(i v_p(2) - v_p(i+1)).$$

Proof. Let $\underline{u} \in U$ and $i > 1$. Replacing u_1 by $u_1^* = u_1 + iu_i$ and u_i by $u_i^* = 0$, we obtain a sequence $\underline{u}^* \in U$ such that:

$$\begin{aligned} v_p(d(\underline{u}^*)) - v_p(d(\underline{u})) &= v_p\left(\frac{(u_1+iu_i)!}{u_1!u_i!}\right) + v_p(2^{iu_i}) - v_p((i+1)^{u_i}) \\ &\geq v_p(2^{iu_i}) - v_p((i+1)^{u_i}) = u_i(i v_p(2) - v_p(i+1)). \quad \square \end{aligned}$$

Lemma 3.2. *If $p = 2$, one has:*

$$\tilde{U}_2 = U_2 = \{(n, 0, \ldots, 0)\},$$
$$A((n, 0, \ldots, 0), m) = \frac{m(m-1)\cdots(m-n+1)}{n!2^n} = \frac{1}{2^n}\binom{m}{n},$$
$$\mu_2 = n + v_2(n!) = \sum_{k \geq 0} \left[\frac{n}{2^k}\right] = \omega_2(n).$$

Proof. The previous lemma shows that

$$v_2(d(\underline{u}^*)) - v_2(d(\underline{u})) \geq u_i(i - v_2(i+1)).$$

For every $i > 1$, one has $i > v_2(i+1)$, and then, $\underline{u} \in U_2$ implies that $u_i = 0$ as soon as $i \neq 1$. All the assertions of the lemma result from this remark. Consequently, Lemma 2.1 shows that $v_2(d(n)) = \omega_2(n)$. $\square$

Lemma 3.3. *If $\underline{u} \in U_p$ and if p divides $i+1$, then either $u_i = 0$ or $i = p-1$.*

Proof. It follows from the previous lemma that we may assume $p \neq 2$. Suppose that there is some $\underline{u} \in U$ and some $i > p-1$ such that p divides $i+1$ and $u_i \neq 0$. The integer i may be written $i = ap^\alpha - 1$ where p does not divide a and either $\alpha \geq 2$ or $\alpha \geq 1$ and $a \geq 2$. Replacing u_1, u_{p-1} and u_i by u_1^*, u_{p-1}^* and u_i^* where

$$u_1^* = u_1 + iu_i - \left[\frac{i}{p-1}\right]u_i, \quad u_{p-1}^* = u_{p-1} + \left[\frac{i}{p-1}\right]u_i; \quad u_i^* = 0,$$

we obtain another sequence $\underline{u}^* \in U$ such that

$$v_p(d(\underline{u}^*)) - v_p(d(\underline{u})) = (v_p(u_1^*!) - v_p(u_1!)) + v_p\left(\left(u_{p-1} + \left[\frac{i}{p-1}\right]u_i\right)!\right)$$

$$- v_p(u_{p-1}!) - v_p(u_i!) + \left[\frac{i}{p-1}\right] u_i - u_i v_p(i+1)$$
$$\geq \left[\frac{i}{p-1}\right] - \alpha.$$

The following inequality

$$\left[\frac{i}{p-1}\right] = \left[\frac{ap^\alpha - 1}{p-1}\right] = a\frac{p^\alpha - 1}{p-1} + \left[\frac{a-1}{p-1}\right] \geq a(1 + p + \cdots + p^{\alpha-1}) \geq a(2\alpha - 1)$$

proves that in all the cases one has $\left[\frac{i}{p-1}\right] > \alpha$. Consequently, $\underline{u} \notin U_p$ since $v_p(d(\underline{u}^*)) > v_p(d(\underline{u}))$. □

Lemma 3.4. *If $\underline{u} \in \tilde{U}_p$, then $u_i = 0$ for every index $i > 1$ such that p does not divide $i + 1$.*

Proof. We may assume $p \neq 2$. Let $\underline{u} \in U$ and $i > 1$ be such that p does not divide $i + 1$. Lemma 3.1 shows that if we replace u_1 by $u_1^* = u_1 + iu_i$ and u_i by $u_i^* = 0$, we obtain a sequence $\underline{u}^* \in U$ such that:

$$v_p(d(\underline{u}^*)) - v_p(d(\underline{u})) \geq v_p(2^{iu_i}) - v_p((i+1)^{u_i}) = 0.$$

If $u_i \neq 0$, one has also $\sigma(\underline{u}^*) - \sigma(\underline{u}) = (i-1)u_i > 0$. Thus, u cannot be in $\tilde{U}_p$. □

Lemma 3.5. *For every $p \in \mathbb{P}$, the subset $\tilde{U}_p$ contains only one sequence and this sequence is of the form*

$$(u_1, 0, \ldots, 0, u_{p-1}, 0, \ldots, 0).$$

Proof. It follows from Lemmas 3.3 and 3.4 that an element $\underline{u}$ of $\tilde{U}_p$ is necessarily of the form $(u_1, 0, \ldots, 0, u_{p-1}, 0, \ldots, 0)$. The unicity results from the relation $u_1 + (p-1)u_{p-1} = n$, since $\sigma(\underline{u}) = u_1 + u_{p-1}$ will then be maximal for only one pair (u_1, u_{p-1}). It remains to prove that $\mu_p = \omega_p(n)$. This will be done in the following lemma. □

Lemma 3.6. *When $(u, v) \in \mathbb{N}^2$ satisfies $u + (p-1)v = n$, the maximum of $v_p(u!v!) + v$ is equal to $\omega_p(n)$.*

Proof. One knows Legendre's formula:

$$v_p(n!) = \sum_{k>0} \left[\frac{n}{p^k}\right].$$

Notice that, for

$$v = \left[\frac{n}{p-1}\right] \quad \text{and} \quad u = n - (p-1)\left[\frac{n}{p-1}\right],$$

one has $0 \leq u < p - 1$, and hence, $v_p(u!) = 0$ and

$$v_p(u!) + v_p(v!) + v = \sum_{k\geq 0} \left[\frac{n}{(p-1)p^k}\right] = \omega_p(n).$$

Consequently, $\mu_p \geq \omega_p(n)$.

Let us show that $\mu_p \leq \omega_p(n)$. Of course, $[\frac{u}{p}] \leq [\frac{u}{p-1}]$, and hence,

$$v_p(u!) = \sum_{k>0} \left[\frac{u}{p^k}\right] \leq \sum_{k\geq 0} \left[\frac{u}{(p-1)p^k}\right].$$

Since $n = u + (p-1)v$, one has

$$\left[\frac{n}{p-1}\right] = \left[\frac{u}{p-1}\right] + v.$$

Then,

$$\omega_p(n) = \sum_{k\geq 0} \left[\frac{n}{(p-1)p^k}\right] \geq \sum_{k\geq 0} \left[\frac{u}{(p-1)p^k}\right] + \sum_{k\geq 0} \left[\frac{v}{p^k}\right] \geq v_p(u!) + v + v_p(v!).$$

□

Remark. It is possible to determine the unique sequence $\underline{u}$ of $\tilde{U}_p$ (when $p \leq n+1$). We know that it suffices to find among the pairs $(u, v) \in \mathbb{N}^2$ such that $u + (p-1)v = n$ and $v_p(u!v!)+v = \omega_p(n)$ the only one such that $u+v$ is maximal. It follows from $[\frac{n}{p-1}] = v+[\frac{u}{p-1}]$ that the equality $v_p(u!v!) + v = \omega_p(n)$ is equivalent to $[\frac{u}{p}] = [\frac{u}{p-1}]$. Thus, if $[\frac{u}{p}] = k$, then $u = (p-1)k+(k+h)$ with $0 \leq h \leq k+h < p-1$. Write $n = (p-1)q+r$ with $0 \leq r < p-1$. Then, $u+(p-1)v = n$ is equivalent to $k+v = q$ and $k+h = r$. Finally, $u+v$ is maximal if and only if u is maximal, that is, if k is maximal, and hence equal to $\inf(q, r)$. If $q \leq r$, then $k = q$, $v = 0$ and $u = n$. If $q > r$, then $k = r$, $h = 0$, $u = pr$ and $v = q - r$. We may summarize: let $n = (p-1)q + r$ with $0 \leq r < p-1$.

Either $q \leq r$, $\underline{u} = (n, 0, \ldots, 0)$ and

$$A(\underline{u}, m) = \frac{m(m-1)\cdots(m-n+1)}{n!2^n}.$$

Or $q > r$, $\underline{u} = (pr, 0, \ldots, 0, q-r, 0, \ldots, 0)$ and

$$A(\underline{u}, m) = \frac{m(m-1)\cdots(m-(p-1)r-q+1)}{(pr)!(q-r)!2^{pr}p^{q-r}}.$$

4. A third sequence of denominators

We have seen that the sequences $\{d(n)\}$ and $\{e(n)\}$ are equal. There are both sequences of denominators: $d(n)$ is the denominator of the polynomial $A_n(m)$, while $e(n)$ is the common denominator of the polynomials of $\mathrm{Int}_{n+1}(\mathbb{P}, \mathbb{Z})$. Let us consider now the sequence $\{\delta(n)\}_{n\in\mathbb{N}}$ where $\delta(n)$ is the denominator of the rational number $\frac{B_n}{n}$ (B_n denotes the n-th Bernoulli number). Bhargava [1, Example 21] noticed the link between the sequences $\{e(n)\}$ and $\{\delta(n)\}$: modulo powers of 2, $e(2n)$ is equal to the product $\prod_{k=1}^{n} \delta(k)$. We are going to make this power of 2 precise.

Recall the definition–notation for the Bernoulli numbers:

$$\frac{z}{e^z - 1} = 1 - \frac{1}{2}z + \frac{B_1}{2!}z^2 - \frac{B_2}{4!}z^4 + \frac{B_3}{6!}z^6 - \cdots$$

Let p be a prime number. Von Staudt's theorem says that, if $p-1$ divides $2n$, then $v_p(B_n) = -1$, and Kummer's theorem says that, if $p-1$ does not divide $2n$, then $v_p(B_n) \geq v_p(n)$.

Consequently, if $\delta(n)$ denotes the denominator of $\frac{B_n}{n}$, then either $p-1$ divides $2n$ and $v_p(\delta(n)) = 1 + v_p(n)$, or $p-1$ does not divide $2n$ and $v_p(\delta(n)) = 0$. Thus,

$$v_p\left(\prod_{k=1}^{n}\delta(n)\right) = \sum_{1\le k\le n,\, p-1|2k}(1+v_p(k)).$$

If $p \neq 2$ and $p-1|2k$, then $v_p(k) = v_p(\frac{2k}{p-1})$. Consequently, for $p \neq 2$,

$$v_p\left(\prod_{k=1}^{n}\delta(n)\right) = \left[\frac{2n}{p-1}\right] + \sum_{1\le k\le\left[\frac{2n}{p-1}\right]} v_p(k) = \left[\frac{2n}{p-1}\right] + v_p\left(\left[\frac{2n}{p-1}\right]!\right) = \omega_p(2n).$$

For $p = 2$,

$$v_2\left(\prod_{k=1}^{n}\delta(n)\right) = \sum_{1\le k\le n}(1+v_2(k)) = n + v_2(n!) = \omega_2(n) = \omega_2(2n) - 2n.$$

Finally,

$$d(2n) = e(2n) = 2^{2n}\prod_{k=1}^{n}\delta(k).$$

Can this last equality explain the previous one?

Acknowledgment

I am grateful to David Adam for several suggestions and especially for the proof of Lemma 3.6.

References

[1] M. Bhargava, The factorial function $\cdots$ and generalizations, Amer. Math. Monthly 107 (2000) 783–799.
[2] J.-L. Chabert, Une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers, Canad. Math. Bull. 39 (1996) 402–407.
[3] J.-L. Chabert, S. Chapman, W. Smith, A basis for the ring of polynomials integer-valued on prime numbers, in: Factorization in Integral Domains, in: Lecture Notes in Pure and Appl. Math., vol. 189, Dekker, New York, 1997, pp. 271–284.
[4] N.J.A. Sloane, The On-Line Encyclopedia in Integer Sequences, http://www.research.att.com/~njas/sequences/index.html.